Cyber security frameworks – which is the right one?

By Christine Antoniou

Choosing a Cyber security framework is a business decision. A structured approach to selecting a security framework starts with understanding the security requirements and risks that are unique to your business and your industry. Many industries including healthcare, government, education and financial have industry specific data security regulations they must adhere to. Other reasons can include legal, compliance, safety; reputation and financial security in case of a serious breach or it can be a differentiator for the organisation by providing confidence to their clients that their services, systems and data are secure.

The decision about which framework to adopt should not be left to the Technology or Security team; boards and senior management need to be involved and responsible.

Security frameworks are designed to help organisations boost their security posture. Such frameworks provide organisations with a common set of practices to follow, as well as a baseline that makes it easier to report on improvements. There are about 250 different security frameworks used globally, developed to suit a wide variety of businesses and sectors.

After discussions with various Cyber security professionals in Australia, their preference came down to NIST 800-53 and ISO 27001/2. These leading frameworks cover the same fundamental building blocks of a security program but differ in some content and layout.

There is no such thing as a one-size-fits-all approach to security, and each framework has its pros and cons. Organisations vary in their complexity and maturity, from small to global conglomerates and governments. For this reason, it is important to research the available security frameworks and balance the benefits and drawbacks of each approach and align to the identified cyber risks for your organisation.

A hybrid framework can help an organisation to meet their unique business objectives and compliance requirements. This approach enables flexibility and ensures continued functionality as the technology and threat landscapes shift. Organisations might opt to become certified in an individual standard such as ISO 27000 or PCI DSS.

Whichever framework or combination of frameworks the organisation selects, the strategy to defend against potential threats while keeping data, systems and technologies secure is important.